На правах рукописи

УДК 510.5, 519.7

Васильев Александр Валерьевич

Эффективные алгоритмы в модели квантовых ветвящихся программ

Специальность: 01.01.09 — дискретная математика и математическая кибернетика

Автореферат

диссертации на соискание ученой степени
кандидата физико-математических наук

Казань – 2009

Работа выполнена на факультете вычислительной математики и кибернетики Казанского государственного университета.

Научный руководитель: доктор физико-математических наук,
профессор Фарид Мансурович Аблаев

Официальные оппоненты: доктор физико-математических наук,
доцент Андрей Анатольевич Вороненко,

доктор физико-математических наук,
доцент Марина Анатольевна Алехина

Ведущая организация: Физико-технологический институт РАН

Защита диссертации состоится 4 июня 2009 года в 14.30 на заседании диссертационного совета Д 212.081.24 при Казанском государственном университете им.В.И.Ульянова-Ленина по адресу: 420008, Казань, ул. Кремлевская, д.18., конференц-зал научной библиотеки им. Н.И.Лобачевского.

С диссертацией можно ознакомиться в научной библиотеке им. Н.И.Лобачевского Казанского государственного университета.

Автореферат разослан _____ 200 г.

Ученый секретарь диссертационного
Совета Д 212.081.24 при КГУ
кандидат физико-математических наук, А.И.Еникеев
доцент

Общая характеристика работы

Актуальность темы исследования. Вычислительные задачи рассматриваются в математической кибернетике с двух встречных направлений. С одной стороны, в области *разработки и анализа эффективных алгоритмов* строятся непосредственные решения задач, что является доказательством их эффективной вычислимости. С другой стороны, целью *теории сложности* является доказательство того, что "трудные" задачи невозможно решить при скромных вычислительных ресурсах. Оба эти направления занимаются оценкой одной и той же величины – алгоритмической сложности вычислительных задач, для которой теория сложности ищет нижние оценки, а теория алгоритмов определяет верхние. В идеальной ситуации верхние и нижние оценки окажутся асимптотически равными, знаменуя нахождение оптимального и полного решения вычислительной задачи. К сожалению, такое происходит довольно редко.

Для построения алгоритмов необходимо зафиксировать некоторую модель вычислений, в терминах которой и будет описываться решение задачи. Такие модели, как машины Тьюринга и схемы из функциональных элементов, предоставляют эту возможность, но доказывать нижние оценки сложности решения некоторой задачи при определенных вычислительных ограничениях оказывается довольно трудно.

Модель ветвящихся программ помимо удобства описания алгоритмов предоставляет подходы для доказательства нижних оценок сложности при некоторых "естественных" ограничениях. В то же время меры сложности ветвящихся программ тесно связаны со сложностью машин Тьюринга и схем из функциональных элементов, что позволяет переносить результаты с одной модели на другую.

Для модели ветвящихся программ наиболее разработанными являются ограничения на порядок и количество считываний входных переменных. Один раз читающая ветвящаяся программа – это ветвящаяся программа с

тем ограничением, что на каждом вычислительном пути каждая переменная встречается не более одного раза. Дополнительное условие "забывания" требует, чтобы считывание всегда происходило в соответствии с фиксированным порядком переменных. Забывающие один раз читающие ветвящиеся программы (используемые при тестировании сверхбольших интегральных схем) называются упорядоченными бинарными диаграммами решений (Ordered Binary Decision Diagrams, сокращенно OBDD).

Учитывая современную тенденцию к уменьшению размера транзисторов, в ближайшем будущем будет достигнут физический предел, после которого в их работе будут проявляться квантовые эффекты. Поэтому актуализируются новые математические модели вычислений.

Предложенная в 80-х годах прошлого века квантовая парадигма вычислений дала новые подходы к определению алгоритмической сложности некоторых вычислительных задач. Например, была показана возможность эффективного вычисления на квантовых компьютерах функций, для которых не доказано существование эффективных алгоритмов в классических моделях. Наиболее известным является алгоритм факторизации Шора, для которого до сих пор неизвестно, существует ли его эффективный классический аналог. В то же время для ряда моделей со специальными ограничениями обнаружены задачи, которые решаются доказательно эффективнее в квантовых моделях по сравнению с классическими.

Отметим, что разработка квантовых компьютеров ставит множество задач как для математиков, так и для инженеров. Причем обе категории исследователей движутся навстречу друг другу: одни разрабатывают быстрые и эффективные по памяти квантовые алгоритмы, а вторые продвигаются в создании полномасштабных квантовых вычислителей, способных устойчиво работать достаточно продолжительное время.

Однако на данный момент вычислители сильно ограничены как по времени жизни системы, так и по числу одновременно доступных кубит. Поэтому реалистичным представляется вариант квантового компьютера, со-

стоящего из небольшого (по памяти) квантового устройства, работающего под управлением классического компьютера. Рассматриваемая нами модель вычислений под названием *квантовые ветвящиеся программы* адекватно описывает упомянутые "квантово-классические" вычисления.

В данной работе мы рассматриваем квантовые один раз читающие ветвящиеся программы полиномиальной ширины (квантовые OBDD, QOBDD), что также соответствует требуемой минимизации квантовых вычислений по времени. Полиномиальная ширина означает логарифмическое ограничение числа кубит для хранения текущего состояния вычислений. Согласно обобщенной нижней оценке ширины квантовых OBDD, логарифмическое число кубит является асимптотически минимальным для многих важных функций.

Таким образом, актуальность работы обоснована как логикой развития теории сложности, так и современным состоянием области построения квантовых вычислителей.

Цель работы. Разработка методов построения эффективных квантовых ветвящихся программ с ограничениями. Применение этих методов для получения более экономных по памяти алгоритмов вычисления булевых функций по сравнению с классическим случаем.

Методы исследований. В работе используются методы дискретной математики, математической кибернетики, теории вероятностей и теории чисел.

Научная новизна. В диссертации получены следующие новые результаты:

1. Предложено представление квантовых ветвящихся программ в виде квантовых схем из функциональных элементов и адаптирована техни-

ка уменьшения вероятности ошибки для квантовых ветвящихся программ.

2. Разработан квантовый метод отпечатков. Он применен для эффективного вычисления индивидуальных функций, представленных в диссертации.

3. Доказано, что квантовые ветвящиеся программы, вычисляющие функции из известного класса NC^1 на одном кубите, являются k раз читающими ветвящимися программами специального вида.

Теоретическая и практическая значимость. Диссертация носит теоретический характер и посвящена исследованиям в области сравнительной сложности классических и квантовых моделей вычислений. Предложенные подходы и разработанные методы могут найти применение при проектировании квантовых вычислителей, в теории сложности квантовых алгоритмов и вычислений.

Апробация работы. Результаты диссертации представлены на российских и международных конференциях и семинарах: IX международном семинаре "Дискретная математика и ее приложения" (Москва, 2007 г.), WACC'07 (Workshop on Algebra, Combinatorics and Complexity, Москва, 2007), XV международной конференции "Проблемы теоретической кибернетики" (Казань, 2008), Workshop on algebra, combinatorics and complexity, CSR 2008 (Москва, 2008), на семинаре ФТИАН (Москва, 2008), на семинаре кафедры математической кибернетики МГУ (Москва, 2008), на семинаре кафедры дискретной математики МГУ (Москва, 2009), на семинарах в университете Турку (Турку, Финляндия, 2007), на итоговых конференциях Казанского государственного университета и на семинарах по классическим и квантовым вычислениям Казанского государственного университета.

Публикации. По теме диссертации опубликовано 6 работ, в том числе 1 – в журнале, входящем в Перечень ВАК.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения и списка литературы из 51 наименования, включая работы автора. Объем диссертации составляет 105 страниц машинописного текста.

Основное содержание работы

В первой главе приводятся основные сведения о детерминированных и вероятностных ветвящихся программах, необходимые для их сравнения с квантовыми аналогами.

Во второй главе рассматривается один из вариантов формализации понятия квантового алгоритма – *квантовые ветвящиеся программы*, ориентированные на вычисление булевых функций.

Введем обозначения, используемые для определения квантовых ветвящихся программ.

Пусть $\mathcal{H}^d$ – d-мерное гильбертово пространство. Разобьем $\mathcal{H}^d$ на прямую сумму двух ортогональных подпространств $\mathcal{H}^d_{accept}$ и $\mathcal{H}^d_{reject}$, где $\mathcal{H}^d_{accept}$ назовем *принимающим* подпространством, а $\mathcal{H}^d_{reject}$ – *отвергающим* подпространством. Будем называть базисные состояния $|i\rangle \in \mathcal{H}^d_{accept}$ принимающими, а $|i\rangle \in \mathcal{H}^d_{reject}$ – отвергающими.

Определение 1. *Квантовая ветвящаяся программа Q над гильбертовым пространством $\mathcal{H}^d$ есть тройка*

$$Q = \langle T, |\psi_0\rangle, M_{accept}\rangle,$$

где T есть последовательность из l инструкций: $T_j = \left(x_{i_j}, U_j(0), U_j(1)\right)$ определяется переменной x_{i_j}, считываемой на шаге j, и унитарными преобразованиями $U_j(0)$ и $U_j(1)$ в пространстве $\mathcal{H}^d$.

Векторы $|\psi\rangle \in \mathcal{H}^d$ *называются состояниями (векторами состояний) программы* Q, $|\psi_0\rangle \in \mathcal{H}^d$ *есть начальное состояние* Q, *а* M_{accept} *– это проектор на принимающее подпространство* $\mathcal{H}^d_{accept}$ *(т.е. диагональная матрица, определяющая проекционное измерение финального состояния).*

Вычисления на входном наборе $\sigma = (\sigma_1, \ldots, \sigma_n) \in \{0,1\}^n$ *происходят следующим образом:*

1. Q *начинает вычисления в исходном состоянии* $|\psi_0\rangle$*;*

2. j*-ая инструкция* Q *считывает переменную* x_{i_j} *и применяет преобразование* $U_j = U_j(\sigma_{i_j})$ *к текущему состоянию* $|\psi\rangle$*, переводящее программу* Q *в состояние* $|\psi'\rangle = U_j(x_{i_j})\,|\psi\rangle$*;*

3. *Конечным состоянием программы является*

$$|\psi(\sigma)\rangle = \left(\prod_{j=l}^{1} U_j(\sigma_{i_j})\right)|\psi_0\rangle \quad .$$

4. *После* l*-го (последнего) шага вычислений измеряется состояние* $|\psi(\sigma)\rangle$*, и набор* σ *принимается с вероятностью*

$$Pr_{accept}(\sigma) = ||M_{accept}\,|\psi_\sigma\rangle\,||_2^2.$$

Шириной квантовой ветвящейся программы Q называется размерность d пространства $\mathcal{H}^d$, а длиной – число l инструкций в последовательности T.

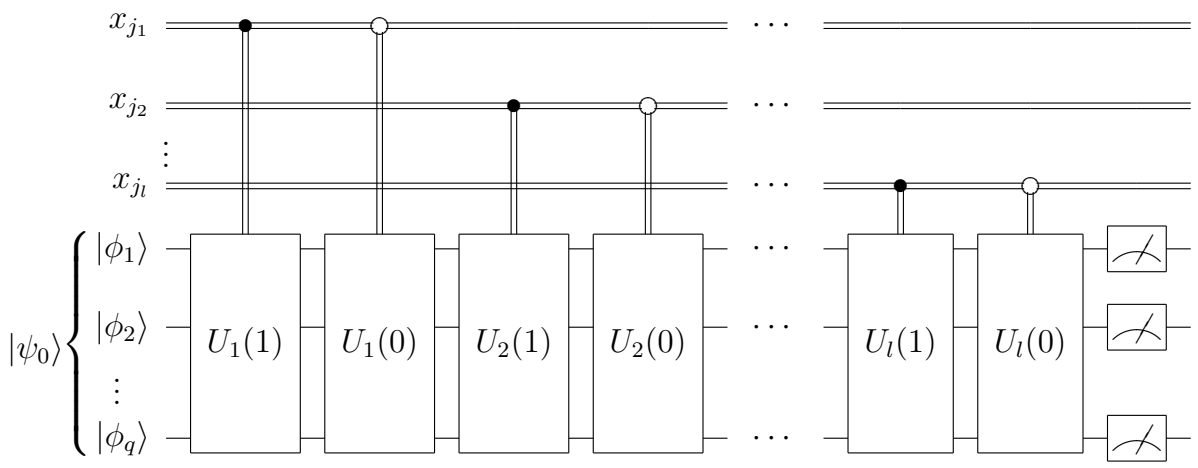
Будем говорить, что квантовая ветвящаяся программа Q *точно вычисляет булеву функцию* f, если для любого набора $\sigma \in f^{-1}(1)$ программа Q заканчивает свою работу в принимающем состоянии, а для любого $\sigma \in f^{-1}(0)$ программа Q заканчивает свою работу в отвергающем состоянии, т.е. вероятность получения правильного ответа равна 1.

Говорят, что квантовая ветвящаяся программа Q *вычисляет булеву функцию* f *с неограниченной ошибкой*, если для любого входного набора $\sigma \in \{0,1\}^n$ выполняется $Pr[Q(\sigma) \neq f(\sigma)] < 1/2$.

Будем говорить, что квантовая ветвящаяся программа Q *вычисляет булеву функцию* f *с односторонней ошибкой*, если существует $\epsilon \in (0,1)$ такое, что для любого $\sigma \in f^{-1}(1)$ вероятность принятия этого набора программой Q равна 1, а для любого $\sigma \in f^{-1}(0)$ вероятность принятия не превышает ϵ.

В диссертации для описанной выше модели предлагается схемное представление, позволяющее наглядно иллюстрировать алгоритмы и вычленять их этапы.

Мы исходим из того, что квантовые ветвящиеся программы можно рассматривать как схемы из функциональных элементов, дополненные возможностью классического управления, т.е. каждый унитарный оператор применяется или не применяется в зависимости от значения соответствующего классического бита.



Здесь $x_{j_1}, \ldots, x_{j_l}$ – последовательность переменных (необязательно различных), обозначающих классические управляющие сигналы, а $|\phi_i\rangle$ образуют регистр квантовых бит (*кубит*). Согласно принятой в литературе по квантовым схемам нотации, классическая информация обозначается на схеме двойными проводами, а квантовая – одиночными.

Заметим, что для квантовой ветвящейся программы в схемном представлении явным образом проявляется еще одна мера сложности – число кубит q, необходимое для физической реализации соответствующей квантовой системы с классическим управлением. Согласно постулатам квантовой

механики для реализации квантовой ветвящейся программы ширины d (системы с d состояниями) потребуется как минимум $\log d$ кубит.

Определение 2. *Назовем квантовую ветвящуюся программу q-кубитной, если она может быть реализована в виде классически управляемой квантовой системы, основанной на q кубитах.*

Далее, в диссертации рассматривается приложение техники уменьшения вероятности ошибки (*probability amplification*) к модели квантовых ветвящихся программ. Показано, что, в отличие от классического вероятностного случая, многократные повторы вычислений, нивелирующие вероятность ошибки, можно производить параллельно, а не последовательно. Это позволяет увеличивать надежность работы квантовых ветвящихся программ без увеличения времени вычислений.

Третья глава описывает предложенный нами метод отпечатков (*fingerprinting*), ориентированный на модель квантовых ветвящихся программ. Техника отпечатков представляет входной набор в виде его образа (*fingerprint*), сохраняющего некоторое свойство входного набора, и позволяет практически достоверно проверять это свойство при измерении квантового состояния.

Техника отпечатков. Для решаемой задачи выбираются целое число $m \geq 2$ и допустимая погрешность $\epsilon \in (0,1)$. Затем фиксируется $t = 2^{\lceil \log((2/\epsilon)\ln 2m)\rceil}$ и строится отображение $g : \{0,1\}^n \to \mathbb{Z}$, описывающее некоторое свойство входного набора.

Далее, для произвольного двоичного набора $\sigma = \sigma_1 \ldots \sigma_n$ порождается его отпечаток $|h_\sigma\rangle$, соединяющий в себе t однокубитных отпечатков $\left|h_\sigma^i\right\rangle$:

$$\begin{aligned} \left|h_\sigma^i\right\rangle &= \cos\tfrac{2\pi k_i g(\sigma)}{m}|0\rangle + \sin\tfrac{2\pi k_i g(\sigma)}{m}|1\rangle \\ |h_\sigma\rangle &= \tfrac{1}{\sqrt{t}}\sum_{i=1}^{t}|i\rangle\left|h_\sigma^i\right\rangle \end{aligned}$$

Другими словами, последний из $\log t + 1$ кубита в квантовом регистре подвергается t различным преобразованиям параллельно. Такой квантовый па-

раллелизм достигается за счет использования контролируемых операторов $C_i(R_i)$, которые применяют вращение R_i к последнему кубиту, если первые $\log t$ кубит находились в состоянии $|i\rangle$, а в противном случае применяется тождественное преобразование I.

Предлагаемая техника нацелена на достоверное распознавание равенства нулю значения $g(\sigma)$. Для этого параметры $k_i \in \{1, \ldots, m-1\}$ для всех $i = \overline{1,t}$ выбираются специальным образом, исходя из следующего определения.

Определение 3. *Множество параметров $K = \{k_1, \ldots, k_t\}$ называется "хорошим" для целого $b \neq 0 \bmod m$, если для некоторого $\epsilon \in (0,1)$*

$$\frac{1}{t^2}\left(\sum_{i=1}^{t} \cos\frac{2\pi k_i b}{m}\right)^2 < \epsilon.$$

Левая часть неравенства при $b = g(\sigma)$ соответствует квадрату амплитуды базисного состояния $|0\rangle^{\otimes \log t}|0\rangle$ после применения оператора $H^{\otimes \log t} \otimes I$ к отпечатку $|h_\sigma\rangle$. Неформально, такое множество гарантирует, что вероятность ошибки будет ограничена величиной ϵ.

Приводится доказательство существования набора необходимых параметров, которое позволяет ограничить вероятность ошибки на всех наборах, где $g(\sigma) \neq 0 \bmod m$:

Лемма 1. *Существует множество K, где $|K| = t = 2^{\lceil \log((2/\epsilon)\ln 2m)\rceil}$, которое является "хорошим" для всех целых $b \neq 0 \bmod m$.*

Рассматриваются варианты применения данной техники, а также ее упрощенный вариант, не использующий запутанных состояний. Эта модификация использует гораздо больше кубит, однако при нынешнем уровне технологий является более пригодной для физической реализации.

Описанная техника отпечатков в совокупности со схемным представлением квантовых ветвящихся программ используется для построения экономных по памяти квантовых ветвящихся программ для следующих булевых функций.

- Функция MOD_m, равная 1 тогда и только тогда, когда число единиц во входном наборе кратно m, где $m \geq 2$ – целое число.

  Предложенная нами квантовая OBDD имеет ширину порядка $\log m$, тогда как в детерминированном случае для вычисления данной функции требуется ширина как минимум m.

- Функция MOD'_m отличается от MOD_m только тем, что входной набор интерпретируется как двоичное число. Поэтому для нее справедливы те же оценки сложности.

- Функция *проверка равенства*:

  $EQ_n(x_1, \ldots, x_n, y_1, \ldots, y_n) = 1$ тогда и только тогда, когда $x_i = y_i$ для всех $i = \overline{1, n}$, т.е. проверяется равенство чисел x и y, заданных соответствующими двоичными последовательностями.

  При наихудшем порядке считывания детерминированная OBDD для данной функции потребует ширины как минимум 2^n, в то время как предложенная нами квантовая OBDD при любом порядке считывания имеет ширину $O(n)$.

- Функция *проверка симметрии* задается следующим образом:

  $Palindrome_n(x_1, \ldots, x_n) = 1 \iff x_1 x_2 \ldots x_{\lfloor n/2 \rfloor} = x_n x_{n-1} \ldots x_{\lceil n/2 \rceil + 1}$. Т.к. данная функция по существу является проверкой равенства, для нее справедливы оценки сложности функции EQ_n.

- Функция *проверка периодичности*, определяемая для целого положительного параметра s следующим образом:

  $Period_n^s(x_0, \ldots, x_{n-1}) = 1$ тогда и только тогда, когда $x_i = x_{i+s \bmod n}$ для всех $i = \overline{0, n-1}$.

  Метод отпечатков позволяет построить квантовую OBDD для данной функции, имеющую ширину $O(n)$.

- Функция *Semi-Simon*, определяемая для целого положительного параметра s следующим образом:

  $Semi\text{-}Simon_n^s(x_0, \ldots, x_{n-1}) = 1$ тогда и только тогда, когда $x_i = x_{i \oplus s}$ для всех $i = \overline{0, n-1}$ (здесь $\oplus$ – это побитовое сложение по модулю 2).

  Для данной функции также удалось построить квантовую OBDD ширины $O(n)$.

- Функция $PERM_n$ проверяет, является ли булевская $n \times n$ матрица перестановочной, т.е. содержащей ровно одну единицу в каждой строчке и каждом столбце.

  Известно, что асимптотическая нижняя оценка ширины любой детерминированной OBDD, вычисляющей данную функцию, есть $2^n n^{-1/2}$ независимо от порядка считывания переменных. Сложность данной функции в классическом вероятностном случае равна $O(n^4 \log n)$. Наш алгоритм дает квантовую ветвящуюся программу ширины $O(n \log n)$. Учитывая, что известная нижняя оценка в квантовом случае асимптотически равна $n - \log n$, предложенный алгоритм почти оптимален.

- Булевский вариант *задачи о скрытой подгруппе*:

  Функция $HSP_{G,K}(x_1, \ldots, x_n) = 1$ тогда и только тогда, когда f, закодированная входным набором, "скрывает" подгруппу K в группе G.

  При помощи метода отпечатков можно вычислить данную функцию квантовой OBDD ширины $O(n)$.

Известные нижние оценки сложности реализации описанных булевых функций в квантовых OBDD показывают, что предложенные ветвящиеся программы являются асимптотически оптимальными по числу кубит.

В заключение рассматривается применение предложенного подхода для вычисления функции голосования $MAJORITY_n$ на одном кубите, а также для решения проблемы равенства в трехсторонней коммуникационной модели (*simultaneous message passing model*, SMP) без общего ключа.

В четвертой главе исследуется структура однокубитных квантовых ветвящихся программ, моделирующих функции из известного класса $\mathbf{NC}^1$.

Баррингтоном в 1989 году была предложена конструкция, позволяющая для произвольной функции из класса $\mathbf{NC}^1$ (класса функций, реализуемых схемами из функциональных элементов логарифмической глубины) построить вычисляющую ее ветвящуюся программу ширины 5, состоящую из последовательности инструкций, выдающих один из двух элементов некоторой неразрешимой группы в зависимости от значения считываемой переменной. Такая программа выдает ответ 0, если произведение выданных элементов есть единица группы, и 1 в противном случае.

В частности, в качестве такой неразрешимой группы можно выбрать группу двумерных унитарных преобразований, описывающих изменение состояния кубита. Таким образом, используя преобразования лишь одного кубита, можно вычислять все функции из класса $\mathbf{NC}^1$.

В работе приводятся необходимые сведения о результатах Баррингтона, и исследуется структура получаемых ветвящихся программ. Далее, описывается моделирование перестановочных ветвящихся программ квантовыми, что позволяет сделать выводы об их структуре. А именно, показано, что они являются $k = n^{O(1)}$ раз читающими квантовыми ветвящимися программами, причем порядок считывания рекурсивно задается конструкцией Баррингтона. Данный результат уточняет метод построения эффективных квантовых ветвящихся программ для функций из класса $\mathbf{NC}^1$ и позволяет сводить исследование классических и квантовых ветвящихся программ константной ширины к исследованию программ, имеющих соответственно ширину 5 и 2 и обладающих описанной структурой.

Благодарности. Автор выражает искреннюю благодарность своему научному руководителю, доктору физико-математических наук, профессору Фариду Мансуровичу Аблаеву за постоянное внимание и неизменную поддержку данной работы.

Публикации по теме диссертации

Работа [1] опубликована в журнале, входящем в Перечень ВАК.

1. **Васильев, А.В. О функциях, вычислимых булевыми схемами логарифмической глубины и ветвящимися программами специального вида / А.В. Васильев // Дискретный анализ и исследование операций. – Серия 1. – 2007. – Т.14, вып. 3. – С. 31–39.**

2. Аблаев, Ф.М. О вычислениях в квантовых ветвящихся программах методом "характерных признаков" / Ф.М. Аблаев, А.В. Васильев // Материалы XV Международной конференции Проблемы теоретической кибернетики (Казань, Россия, 2–7 июня, 2008). – Казань: Изд-во "Отечество", 2008. – С. 1.

3. Васильев, А.В. Соотношение классов NC^1 и *poly*-OBDD$_5$ / А.В. Васильев // Материалы IX международного семинара "Дискретная математика и приложения". – М.: Изд-во механико-математического факультета МГУ, 2007. – С. 68-71.

4. Ablayev, F.M. On Complexity of Quantum Branching Programs Computing Equality-like Boolean Functions / F.M. Ablayev, A.F. Khasianov, A.V. Vasiliev // Electronic Colloquium on Computational Complexity (http://www.eccc.uni-trier.de/eccc/). – TR08-085, 2008.

5. Ablayev, F.M. On the Computation of Boolean Functions by Quantum Branching Programs via Fingerprinting / F.M. Ablayev, A.V. Vasiliev // Electronic Colloquium on Computational Complexity (http://www.eccc.uni-trier.de/eccc/), TR08-059. – 2008.

6. Vasiliev, A.V. Functions computable by Boolean circuits of logarithmic depth and branching programs of a special type / A.V. Vasiliev // Journal of Applied and Industrial Mathematics. – 2008. – Vol. 2. – No. 4. – P. 585-590.